

Common Vulnerabilities and Exposures — CVE®

The Standard for Information Security Vulnerability Names

CVE is a dictionary of common names for publicly known information security vulnerabilities. CVE's common identifiers—called CVE Identifiers—make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

CVE is:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- The way for disparate databases and tools to “speak” the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use
- Industry-endorsed via the CVE Editorial Board and CVE-Compatible Products

Why CVE

CVE was launched in 1999 when most information security tools used their own databases with their own names for security vulnerabilities. At that time there was no significant variation among products and no easy way to determine when the different databases were referring to the same problem. The consequences were potential gaps in security coverage and no effective interoperability among the disparate databases and tools. In addition, each tool vendor used different metrics to state the number of vulnerabilities or exposures they detected, which meant there was no standardized basis for evaluation among the tools.

CVE's common, standardized identifiers provided the solution to these problems. CVE is now the industry standard for vulnerability names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other. They also provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's

needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

How CVE Works

The process of creating a CVE Identifier begins with the discovery and report of a potential security vulnerability. The information is then assigned a CVE Identifier by a CVE Numbering Authority (CNA) and posted on the CVE List on the CVE Web site by the CVE Editor. As part of its management of CVE, The MITRE Corporation functions as Editor and Primary CNA. The CVE Editorial Board oversees this process.

CVE in Use

As the industry standard, CVE Identifiers are used in numerous information security products and services from around the world. These “CVE-Compatible” products include vulnerability databases; security advisories and archives; vulnerability notification, assessment, and remediation products; intrusion detection, management,



The MITRE Corporation maintains CVE and its public Web site, manages the compatibility program, and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure CVE serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org

MITRE

monitoring, and response products; incident management products; data/event correlation products; educational materials; firewalls; patch management products; policy compliance products; and security information management tools.

The U.S. National Vulnerability Database (NVD) of CVE fix information (<http://nvd.nist.gov>)—sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security and operated by the National Institute of Standards and Technology (NIST)—is based on and synchronized with the CVE List. NVD also includes Security Content Automation Protocol (SCAP) mappings for CVE-IDs. SCAP is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance) and CVE is one of the open community standards SCAP uses for enumerating, evaluating, and measuring the impact of software problems and reporting results. The use of CVE by U.S. agencies was also recommended by NIST in two official documents in 2002, and in June 2004, the U.S. Defense Information Systems Agency (DISA) issued a task order for information assurance applications that requires the use of products that use CVE Identifiers.

CVE also helped to create new initiatives: MITRE's Common Weakness Enumeration (CWE™) dictionary of software weaknesses is based in part on the 55,000+ CVE Identifiers on the CVE List, and its Open Vulnerability and Assessment Language (OVAL®), a community-developed language for determining vulnerability and configuration issues on computer systems using community-developed XML schemas and definitions, bases its OVAL Vulnerability Definitions primarily on CVE Identifiers.

And in 2011, the International Telecommunication Union's (ITU-T) Cybersecurity Rapporteur Group, which is the telecom/information system standards body within the treaty-based 150-year-old intergovernmental organization, adopted CVE as a part of its "Cybersecurity Information Exchange Framework (X.CYBIEF)" by issuing *Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures*

Each CVE Identifier Includes

- CVE Identifier number (i.e., "CVE-1999-0067").
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

(CVE), that is based upon CVE's current Compatibility Requirements, and any future changes to the document will be reflected in subsequent updates to X.CVE.

CVE Community

CVE is an international information security community effort. In addition to the contributions of the CVE Editorial Board and the CVE Sponsor, numerous organizations from around the world have made their products CVE-Compatible, have included CVE Identifiers in their security advisories, and/or have adopted or promoted the use of CVE.

CVE Editorial Board The CVE Editorial Board, which includes members from numerous information security-related organizations from around world such as commercial security tool vendors, members of academia, research institutions, government agencies, and other prominent security experts, oversees which vulnerabilities or exposures are included in the CVE List.

CVE Sponsor CVE is sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

CVE-Compatible Products and Services Numerous organizations from around the world have made their information security products and services "CVE-Compatible" by incorporating CVE Identifiers. Refer to the CVE Compatibility section of the CVE Web site for a list of official CVE-Compatible Products and Services and Declarations to Be CVE-Compatible.